УДК 004.056.5

РАЗРАБОТКА УСТРОЙСТВА ДЛЯ ОБМЕНА ЗАКРЫТОЙ ДОКУМЕНТАЛЬНОЙ ИНФОРМАЦИЕЙ ПО ПРОМЫШЛЕННЫМ СЕТЯМ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ

Дрозд О.В.,
научный руководитель канд. техн. наук Капулин Д.В.
Институт космических и информационных технологий
Сибирского федерального университета

Широкое распространение технологий беспроводного *Ethernet* в корпоративном секторе и в секторе электронных устройств для частного пользования закономерным образом привело к росту внимания к этим технологиям со стороны производителей и интеграторов автоматизированных систем управления технологическими процессами (АСУ ТП). Применительно к АСУ ТП, беспроводные сети обладают такими преимуществами как возможность расположения устройств приема-передачи данных в труднодоступных местах, оперативность и удобство развертывания и обслуживания системы, возможность добавления и исключения количества устройств в сети.

Кроме того, внедрение беспроводных устройств контроля параметров открывает новые области для применения систем автоматики, контроля и управления, такие как обеспечение доступа к системам объекта, контроль периметра объекта, наблюдение за перемещениями персонала на территории предприятия, автоматизация контроля проведения инспекций и технического обслуживания, контроль экологических параметров окружающей среды.

При этом, по сути, единственным сдерживающим фактором для широкого распространения беспроводных сетей, в частности, сетей стандарта *IEEE* 802.11, является низкий уровень защищенности каналов связи и недостаточная надежность используемых в настоящий момент алгоритмов шифрования данных, таких как *Triple-DES*и *AES*.

Цель данной работы была поставлена следующим образом: необходимо обеспечить безопасную передачу данных по промышленным беспроводным сетям передачи данных с использованием российских стандартов шифрования данных при работе с устройствами (в том числе и с мобильными устройствами) сторонних производителей. Задачей, поставленной в ходе данной работы, является разработка и реализация криптографического блока на базе программируемой логической интегральной схемы (ПЛИС) с помощью языка описания аппаратуры *Verilog*, разработка отладочного комплекса с использованием серийного комплекта разработчика на базе ПЛИС *XilinxSpartan*-6 и набора отладочных модулей, представляющих собойключевые узлы конечного устройства.

На рис. 1 изображена структурная схема устройства обмена закрытой документальной информацией. Для защиты канала передачи данных необходимо как минимум два подобных устройства, одно из которых связано с передатчиком и выполняет шифрование передаваемых данных, второе устройство связано с приемником и предназначено для дешифрования полученных данных. При этом данные устройства аналогичны и взаимозаменяемы.

В состав устройства (1) входят следующие компоненты: проводной *USB* интерфейс (2); преобразователь интерфейсов *USB*/*UART* (3); криптографический блок на базе ПЛИС (4); радиоинтерфейс *IEEE* 802.11 (5) с встроенной радиоантенной (7); энергонезависимая память (8); программатор энергонезависимой памяти (9); проводной *RS*-232 интерфейс (10); аккумуляторная батарея (11), источник электропитания (12); переклю-

чатель режимов работы (13), генератор тактовых импульсов (14). Также возможно подсоединение внешней радиоантенны (6).

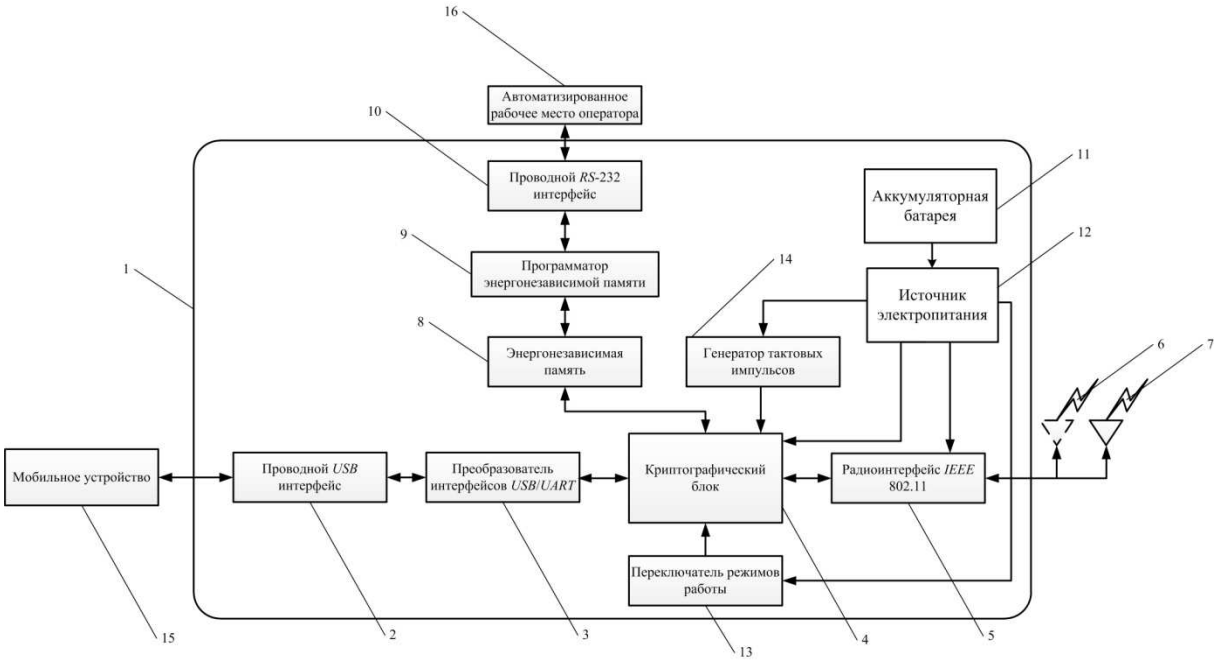

Рис. 1. Структурная схема устройства обеспечения защищенной передачи данных

Отладочный комплекс (рис. 2) состоит из серийного комплекта разработчика на базе ПЛИС *XilinxSpartan*-6 в виде отладочной платы и четырех отладочных модулей, представляющих собой ключевые узлы конечного устройства. В состав отладочного комплекса входят модуль проводного интерфейса *USB*; модуль радиоинтерфейса*IEEE* 802.11; модуль, включающий в себя ключевое запоминающее устройство (КЗУ) и адаптер перепрограммирования КЗУ; модуль, включающий в себя аккумуляторную батарею, блок питания, блок зарядки аккумуляторной батареи.

Рис. 2. Структурная схема отладочного комплекса.

Модуль проводного интерфейса основан на преобразователе интерфейсов*USB-UARTFT*232*RL*.Модуль радиоинтерфейса основан на модуле радиоинтерфейса *WizFi* 220 со встроенной антенной. Также к данному модулю возможно подключение внешней антенны.В качестве ключевого запоминающего устройства используется микросхема электрически стираемого перепрограммируемого постоянного запоминающего устройства 24*LC*02 емкостью 2048 бит, что позволяет хранить восемь секретных ключей по 256 бит каждый.В качестве аккумуляторных батарей используются два литий-ионных аккумулятора форм-фактора 18650 емкостью по 3200 мА·ч, для управления процессом заряжания аккумуляторных батарей используется контроллер заряда *bq*24002, для преобразования напряжения питания используются два преобразователя напряжения *MAX*1674.

В состав криптографического блока входят два программных приемопередатчика стандарта *UART*, обеспечивающие взаимодействие между криптографическим блоком и внешними устройствами, управляющий процессор и блоки шифрования и дешифрования данных, реализующие соответствующие функции алгоритма криптографического преобразования ГОСТ 28147-89.Структура криптографического блока представлена на рис. 3.

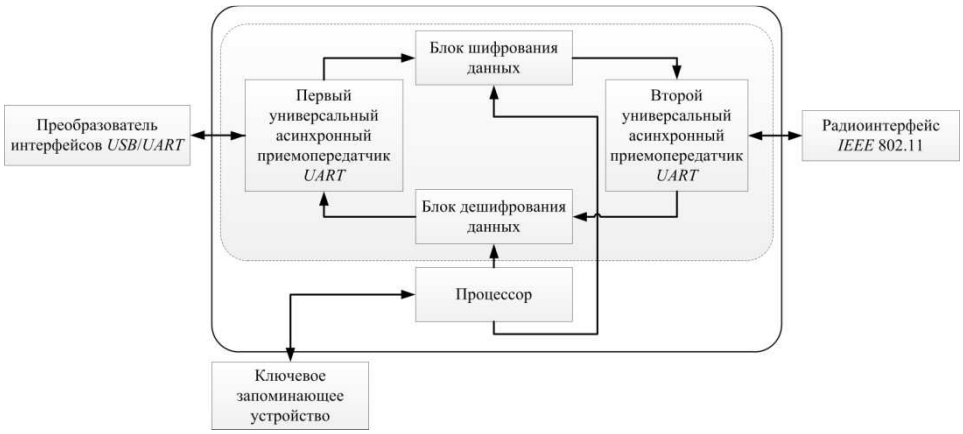

Рис. 3. Структурная схема криптографического блока

Криптографический блок выполнен на базе ПЛИС и обеспечивает реализацию всех основных режимов работы шифроалгоритма ГОСТ 28147-89: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки. Реализация режимов работы шифроалгоритма выполнена на языке описания аппаратуры *Verilog*. Для аппаратной реализации рекомендуется ПЛИС *Spartan*-6 (производитель *Xilinx*, США).

В таблице 1 представлены некоторые параметры реализации шифроалгоритма ГОСТ 28147-89 на базе ПЛИС, в данном случае представлены параметры реализации 32-х раундов шифрования данных в режиме простой замены.

Таблица 2 – Параметры реализации шифроалгоритма ГОСТ 28147-89 на базе ПЛИС

Семейство ПЛИС	Модель ПЛИС	Логических ячеек	Задержка, нс	Потребляемая мощность	Частота, МГц	Пропускная способность, Мб/с
Artix-7	*XC7A*200	3808	131,0860	0,0730	7,6286	61,0286
Spartan-6	*XC6SLX*25	3808	161,3270	0,0290	6,1986	49,5887
	*XC6SLX*150			0,1130		

Моделирование устройства в среде *Simulink* показало, что устройство обеспечивает надежную обработку и передачу данных в совокупности с такими интерфейсами, как *IEEE* 802.11*ac*, *FastEthernet*, *GigabitEthernet*. В ходе моделирования устройство была представлено в виде трехканальной (три потока шифрования) системы массового обслуживания. Результаты моделирования представлены в таблице 2.

Таблица 2 – Результаты моделирования устройства для обмена закрытой документальной информацией

Стандарт	Время работы СМО, мкс	Поступило заявок	Обслужено заявок	Не обслужено заявок
802.11*g*	100	56	56	0
802.11*n*	100	156	156	0
802.11*ac*	100	1364	1362	2
GigabitEthernet	100	1040	1038	2
FastEthernet	100	104	104	0
USB 1.0	100	12	12	0
USB 2.0	100	498	497	1
USB 3.0	100	1915	1872	43

Также возможно использование системы с устройствами с интерфейсом *USB* 3.0 при использовании промежуточных накопителей для поступающих пакетов данных.

Таким образом, предлагаемоеустройство для обмена закрытой документальной информацией позволяет решать задачу обеспечения защищенной передачи данных по промышленным сетям беспроводной передачи данных с использованием стандарта шифрования данных ГОСТ 28147-89, а также способно обеспечивать защиту беспроводной передачи данных между любыми другими устройствами, поддерживающими интерфейсы *USB* и *Wi-Fi*.